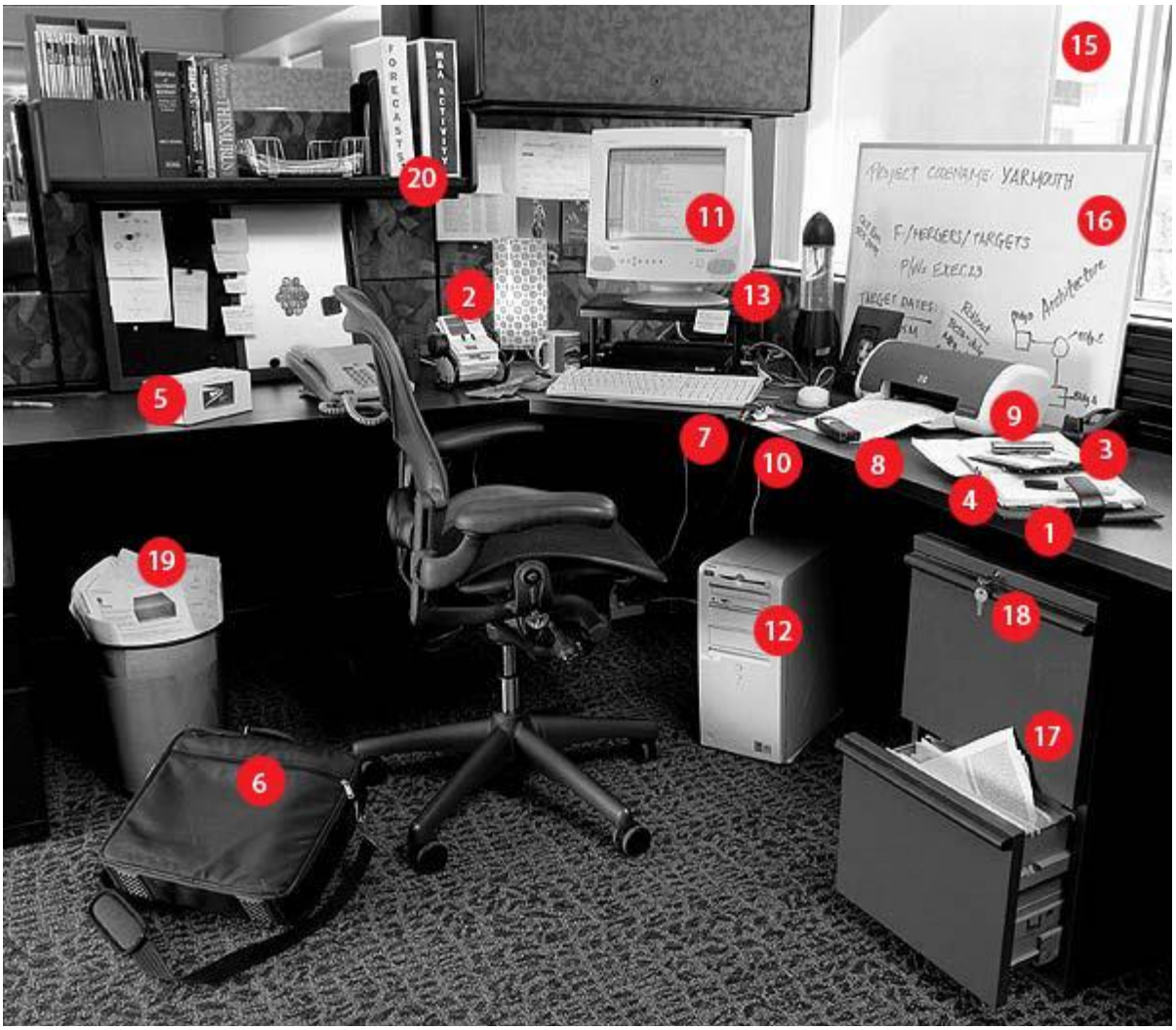
Clean Desk Answer Key



Proprietary Data

Violations	Risk	Suggested Policy
Day planner **(1)** and Rolodex **(2)** left on desk.	Personal and professional information—including phone numbers, passwords, or notes on meeting times, places and subjects—is vulnerable.	Store day planners and notebooks in a locked drawer or take them when away from desk for extended periods of time, including overnight.

Clean Desk Answer Key

Personal Data

Violations	Risk	Suggested Policy
Personal effects including a bank statement **(3)**, checkbook **(4)** and mail **(5)** left on desk. Briefcase **(6)** left open near desk.	Bank statements include account numbers and other personal identifiers; mail carries home addresses and could reveal private information; checkbook contains a history of financial transactions. Unlocked briefcases can have items stolen from them if employee leaves the area.	• Lock briefcases and cabinets when away from desk for extended periods. • Keep all personal effects in a locked briefcase or locked cabinet devoted to personal effects.

Access Tools

Violations	Risk	Suggested Policy
Keys **(7)**, cell phone **(8)**, PDA **(9)** and building access card **(10)** left on desk.	Cell phones can be stolen or have their call histories compromised. Stolen keys give intruders access to restricted areas of the office. PDAs contain sensitive personal and professional data. Stolen access cards can be used for continued access to the building.	• Keep devices with you, and lock cell phones and PDAs with a pass code. • Never leave your access cards or keys out anywhere; always keep them with you. • Notify security staff immediately if access cards or keys are missing.

IT Tools

Violations	Risk	Suggested Policy
Applications left open on computer **(11)**, CD left in computer **(12)**, passwords on sticky note displayed on monitor stand **(13)**, and printouts left in printer **(14)**.	Access to personal or sensitive corporate e-mail or passwords can allow ongoing access and intrusion. CD left in drive and data on printouts can be stolen. Cache files for applications and printer can yield sensitive data one might have thought weren't preserved.	• Close applications and turn off your monitor when you leave your desk. • Do not leave portable media such as CDs or floppy disks in drives. • Enable a password-protected screen saver. • Turn off your computer when you leave for extended periods. • Never write your passwords on a sticky note nor try to hide them anywhere in your office. • Remove printouts from printers before leaving your office. • Shred sensitive printouts when you are done with them. • Clear cache files on computer and memory on devices like printers regularly.

Spatial Misconfigurations

Violations	Risk	Suggested Policy
Desk positioned so it's partially exposed to window and view from the hallway **(15)**. Whiteboard with sensitive data on it viewable from hallway and window **(16)**.	Window exposure could enable spying from other buildings. Hallway exposure could allow unauthorized access if data, such as a password, is written on a whiteboard.	• Desks and furniture should be positioned so that sensitive material is not visible from either the windows or the hallway. • Close blinds on windows. • Use a screen filter to minimize the viewing angle on a computer monitor. • Erase whiteboards; if data on whiteboards needs to be saved, use electronic whiteboards or employ shutters.

Beyond Desk

Violations	Risk	Suggested Policy
File cabinet drawer open **(17)** and keys left in lock **(18)**. Trash bin contains loose-leaf paper **(19)**. Bookshelf contains binders with sensitive information **(20)**.	Folders in cabinet are eminently stealable. Keys allow for ongoing access and the ability to return files, so it's hard to detect theft. E-mails, other sensitive paper in trash bin can be stolen after-hours or found in the Dumpster outside. Binders on shelf, clearly marked as sensitive, are also available for	• Do not use bookshelves to store binders with sensitive information. Label those binders prosaically and lock them up. • Arrange folders in file cabinets so that the least sensitive are in front, most sensitive in back. • Keep file cabinets closed

	"borrowing," making the theft of the information hard to detect.	and locked. Do not leave keys in their locks. • Shred paper before throwing it away. Participate in a corporate wide shredding program. • Lock your office door when you're gone for extended periods.